6712-01

This document is scheduled to be published in the Federal Register on 11/23/2022 and available online at **federalregister.gov/d/2022-25263**, and on **govinfo.gov**

FEDERAL COMMUNICATIONS COMMISSION

47 CFR Parts 10 and 11

[PS Docket Nos. 15-94, 15-91, 22-329; FCC 22-82; FR ID 113410]

Emergency Alert System; Wireless Emergency Alerts; Protecting the Nation's Communications Systems from Cybersecurity Threats

AGENCY: Federal Communications Commission.

ACTION: Proposed rule.

SUMMARY: In this document, the Commission proposes requirements for Emergency Alert System (EAS) Participants to report compromises of their EAS equipment, communications systems, and services to the Commission. Additionally, this document proposes requirements for EAS Participants and Commercial Mobile Service (CMS) providers that participate in Wireless Emergency Alerts (WEA) to annually certify to having a cybersecurity risk management plan in place and to employ sufficient security measures to ensure the confidentiality, integrity, and availability of their respective alerting systems. This document also proposes requirements for participating CMS providers to take steps to ensure that only valid alerts are displayed on consumer devices. These requirements would further protect the nation's communications systems from cybersecurity threats. With this Notice of Proposed Rulemaking, the Commission seeks comment on the proposed rules and any suitable alternatives.

DATES: Comments are due on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]** and reply comments are due on or before **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].**

ADDRESSES: You may submit comments, identified by PS Docket Nos. 15-94, 15-91, and 22-329, by any of the following methods:

- *Electronic Filers*: Comments may be filed electronically using the Internet by accessing the ECFS: http://apps.fcc.gov/ecfs/.
- *Paper Filers*: Parties who choose to file by paper must file an original and one copy of each filing.

  Filings can be sent by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission.

  - Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9050 Junction Drive, Annapolis Junction, MD 20701.
  - U.S. Postal Service first-class, Express, and Priority mail must be addressed to 45 L Street NE, Washington, DC 20554.
- Effective March 19, 2020, and until further notice, the Commission no longer accepts any hand or messenger delivered filings. This is a temporary measure taken to help protect the health and safety of individuals, and to mitigate the transmission of COVID-19. *See FCC Announces Closure of FCC Headquarters Open Window and Change in Hand-Delivery Policy*, Public Notice, DA 20-304 (March 19, 2020). https://www.fcc.gov/document/fcc-closes-headquarters-open-window-and-changes-hand-delivery-policy.

People with Disabilities. To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at 202-418-0530 (voice), 202-418-0432 (tty).

FOR FURTHER INFORMATION CONTACT: For further information regarding Notice of Proposed Rulemaking, please contact James Wiley, Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau, (202) 418-1678, or by email to James.Wiley@fcc.gov, or Steven Carpenter, Cybersecurity and Communications Reliability

Division, Public Safety and Homeland Security Bureau, (202) 418-2313, or by email to Steven.Carpenter@fcc.gov. For additional information concerning the Paperwork Reduction Act information collection requirements contained in this document, send an email to PRA@fcc.gov or contact **Nicole Ongele, Office of Managing Director, Performance Evaluation and Records Management, 202-418-2991, or by email to** PRA@fcc.gov.

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's Notice of Proposed Rulemaking (*NPRM*), in PS Docket Nos. 15-94, 15-91, 22-329; FCC 22-82, adopted and released on October 27, 2022. The full text of this document is available by downloading the text from the Commission's website at: https://docs.fcc.gov/public/attachments/FCC-22-82A1.pdf.

Paperwork Reduction Act

This Notice of Proposed Rulemaking (*NPRM*) seeks comment on potential new or revised proposed information collection requirements. If the Commission adopts any new or revised final information collection requirements when the final rules are adopted, the Commission will publish a notice in the *Federal Register* inviting further comments from the public on the final information collection requirements, as required by the Paperwork Reduction Act of 1995, Public Law 104-13 (44 U.S.C. 3501-3520). The Commission, as part of its continuing effort to reduce paperwork burdens, invites the general public and OMB to comment on the information collection requirements contained in this document, as required by the PRA. Public and agency comments on the PRA proposed information collection requirements are due **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].** Comments should address: (a) whether the proposed collection of information is necessary for the proper performance of the functions of the Commission, including whether the information shall have practical utility; (b) the accuracy of the Commission's burden estimates; (c) ways to enhance the quality, utility, and clarity of the information collected; (d) ways to minimize the burden of the collection of information on the respondents, including the use of automated

collection techniques or other forms of information technology; and (e) way to further reduce the information collection burden on small business concerns with fewer than 25 employees. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, Pub. L. 107-198, see 44 U.S.C. 3506(c)(4), we seek specific comment on how we might further reduce the information collection burden for small business concerns with fewer than 25 employees.

I. Initial Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA), the Commission has prepared this Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on a substantial number of small entities by the policies and rules proposed in the *NPRM*. Written public comments are requested on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comments on the *NPRM*. The Commission will send a copy of the *NPRM*, including this IRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA). In addition, the *NPRM* and IRFA (or summaries thereof) will be published in the *Federal Register*.

A. Need for, and Objectives of, the Proposed Rules

2. The *NPRM* raises awareness concerning security of the nation's alert and warning systems is essential to helping safeguard the lives and property of all Americans. To ensure that the EAS and WEA remain strong, the Commission must act proactively in its oversight of stakeholders associated with these systems. The Commission has previously encouraged stakeholders to ensure that their systems are secure and provided guidance on specific steps that communications providers could take to secure their equipment. According to data collected by the Public Safety and Homeland Security Bureau (Bureau) during the nationwide EAS test in August 2021 however, more than 5,000 EAS Participants were using outdated software or using equipment that no longer supported regular software updates. Moreover, in the area of equipment operational readiness, the test also revealed that an appreciable number of EAS Participants were unable to participate in testing due to equipment failure. This was despite

receiving advanced notice that the test was going to be conducted. The Commission therefore believes the information revealed in the nationwide EAS test signals that we should take action to ensure and enhance the security of the EAS and WEA. In the *NPRM*, the Commission acts to improve the security and reliability of the EAS and WEA by proposing and seeking comment on rules promoting the operational readiness of EAS equipment, improving awareness of unauthorized access to EAS equipment, communications systems, or services, protecting the nation's alerting systems through the development, implementation, and certification of a cybersecurity risk management plan and displaying only valid WEA messages on mobile devices.

3. The *NPRM* includes specific proposals upon which the Commission seeks comment include: requiring EAS Participants and Participating CMS Providers to annually certify to having a cybersecurity risk management plan in place and employing sufficient security controls to ensure the confidentiality, integrity, and availability of their respective alerting systems (including certain baseline security controls); requiring EAS Participants to report any incident of unauthorized access of their EAS equipment, communications systems, or services (i.e., regardless of whether that compromise has resulted in the transmission of a false alert) to the Commission via NORS within 72 hours of when it knew or should have known that an incident has occurred, and provide details concerning the incident and requiring that mobile devices only present WEA alerts from valid base stations. In addition, the Commission seeks comment on whether and how to promote the operational readiness of EAS. The Commission also seeks comment to refresh the record on previously proposed changes to the WEA infrastructure functionality rules, and on how our proposals in the *NPRM* may promote or inhibit advances in diversity, equity, inclusion, and accessibility, as well as on the scope of the Commission's relevant legal authority.

B. Legal Basis

4. The proposed action is authorized pursuant to sections 1, 2, 4(i), 4(n), 301, 303(b), 303(g), 303(r), 303(v), 307, 309, 335, 403, 624(g), and 706 of the Communications Act of 1934, as amended, 47 U.S.C. 151, 152, 154(i), 154(n), 301, 303(b), 303(g), 303(r), 303(v), 307, 309, 335, 403, 544(g), and 606; The Warning, Alert and Response Network (WARN) Act, WARN Act sections 602(a), (b), (c), (f), 603, 604, and 606, 47 U.S.C. 1202(a),(b),(c), (f), 1203, 1204 and 1206; the Wireless Communications and Public Safety Act of 1999, Pub. L. 106-81, 47 U.S.C. 615, 615a, 615b; Section 202 of the Twenty-First Century Communications and Video Accessibility Act of 2010, as amended, 47 U.S.C. 613.

C. Description and Estimate of the Number of Small Entities to Which the Proposed Rules Will Apply

5. The RFA directs agencies to provide a description of and, where feasible, an estimate of, the number of small entities that may be affected by the proposed rules, if adopted. The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction." In addition, the term "small business" has the same meaning as the term "small business concern" under the Small Business Act. A "small business concern" is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the Small Business Administration (SBA).

6. *Small Businesses, Small Organizations, Small Governmental Jurisdictions*. Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe here, at the outset, three broad groups of small entities that could be directly affected herein. First, while there are industry specific size standards for small businesses that are used in the regulatory flexibility analysis, according to data from the SBA's Office of Advocacy, in general a small business is an independent business having fewer than 500 employees. These types of small businesses represent 99.9% of all businesses in the United States, which translates to 32.5 million businesses.

7. Next, the type of small entity described as a "small organization" is generally "any not-for-profit enterprise which is independently owned and operated and is not dominant in its field." The Internal Revenue Service (IRS) uses a revenue benchmark of $50,000 or less to delineate its annual electronic filing requirements for small exempt organizations. Nationwide, for tax year 2020, there were approximately 447,689 small exempt organizations in the U.S. reporting revenues of $50,000 or less according to the registration and tax data for exempt organizations available from the IRS.

8. Finally, the small entity described as a "small governmental jurisdiction" is defined generally as "governments of cities, counties, towns, townships, villages, school districts, or special districts, with a population of less than fifty thousand." U.S. Census Bureau data from the 2017 Census of Governments indicate that there were 90,075 local governmental jurisdictions consisting of general purpose governments and special purpose governments in the United States. Of this number there were 36,931 general purpose governments (county, municipal and town or township) with populations of less than 50,000 and 12,040 special purpose governments - independent school districts with enrollment populations of less than 50,000. Accordingly, based on the 2017 U.S. Census of Governments data, we estimate that at least 48,971 entities fall into the category of "small governmental jurisdictions."

9. *Wireless Telecommunications Carriers (except Satellite)*. This industry comprises establishments engaged in operating and maintaining switching and transmission facilities to provide communications via the airwaves. Establishments in this industry have spectrum licenses and provide services using that spectrum, such as cellular services, paging services, wireless internet access, and wireless video services. The SBA size standard for this industry classifies a business as small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2017 show that there were 2,893 firms in this industry that operated for the entire year. Of that number, 2,837 firms employed fewer than 250 employees. Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020,

there were 797 providers that reported they were engaged in the provision of wireless services. Of these providers, the Commission estimates that 715 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

10. *Broadband Personal Communications Service*. The broadband personal communications services (PCS) spectrum encompasses services in the 1850-1910 and 1930-1990 MHz bands. The closest industry with a SBA small business size standard applicable to these services is Wireless Telecommunications Carriers (*except* Satellite). The SBA small business size standard for this industry classifies a business as small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2017 show that there were 2,893 firms that operated in this industry for the entire year. Of this number, 2,837 firms employed fewer than 250 employees. Thus under the SBA size standard, the Commission estimates that a majority of licensees in this industry can be considered small.

11. Based on Commission data as of November 2021, there were approximately 5,060 active licenses in the Broadband PCS service. The Commission's small business size standards with respect to Broadband PCS involve eligibility for bidding credits and installment payments in the auction of licenses for these services. In auctions for these licenses, the Commission defined "small business" as an entity that, together with its affiliates and controlling interests, has average gross revenues not exceeding $40 million for the preceding three years, and a "very small business" as an entity that, together with its affiliates and controlling interests, has had average annual gross revenues not exceeding $15 million for the preceding three years. Winning bidders claiming small business credits won Broadband PCS licenses in C, D, E, and F Blocks.

12. In frequency bands where licenses were subject to auction, the Commission notes that as a general matter, the number of winning bidders that qualify as small businesses at the close of an auction does not necessarily represent the number of small businesses currently in

service. Further, the Commission does not generally track subsequent business size unless, in the context of assignments or transfers, unjust enrichment issues are implicated. Additionally, since the Commission does not collect data on the number of employees for licensees providing these, at this time we are not able to estimate the number of licensees with active licenses that would qualify as small under the SBA's small business size standard.

13. *Narrowband Personal Communications Services*. Narrowband Personal Communications Services (*Narrowband PCS*) are PCS services operating in the 901-902 MHz, 930-931 MHz, and 940-941 MHz bands. PCS services are radio communications that encompass mobile and ancillary fixed communication that provide services to individuals and businesses and can be integrated with a variety of competing networks. Wireless Telecommunications Carriers (*except* Satellite) is the closest industry with a SBA small business size standard applicable to these services. The SBA small business size standard for this industry classifies a business as small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2017 show that there were 2,893 firms that operated in this industry for the entire year. Of this number, 2,837 firms employed fewer than 250 employees. Thus under the SBA size standard, the Commission estimates that a majority of licensees in this industry can be considered small.

14. According to Commission data as of December 2021, there were approximately 4,211 active *Narrowband PCS* licenses. The Commission's small business size standards with respect to *Narrowband PCS* involve eligibility for bidding credits and installment payments in the auction of licenses for these services. For the auction of these licenses, the Commission defined a "small business" as an entity that, together with affiliates and controlling interests, has average gross revenues for the three preceding years of not more than $40 million. A "very small business" is defined as an entity that, together with affiliates and controlling interests, has average gross revenues for the three preceding years of not more than $15 million. Pursuant to these definitions, 7 winning bidders claiming small and very small bidding credits won approximately 359 licenses. One of the winning bidders claiming a small business status

classification in these *Narrowband PCS* license auctions had an active license as of December 2021.

15. In frequency bands where licenses were subject to auction, the Commission notes that as a general matter, the number of winning bidders that qualify as small businesses at the close of an auction does not necessarily represent the number of small businesses currently in service. Further, the Commission does not generally track subsequent business size unless, in the context of assignments or transfers, unjust enrichment issues are implicated. Additionally, since the Commission does not collect data on the number of employees for licensees providing these services, at this time we are not able to estimate the number of licensees with active licenses that would qualify as small under the SBA's small business size standard.

16. *Wireless Communications Services*. Wireless Communications Services (WCS) can be used for a variety of fixed, mobile, radiolocation, and digital audio broadcasting satellite services. Wireless spectrum is made available and licensed for the provision of wireless communications services in several frequency bands subject to Part 27 of the Commission's rules. Wireless Telecommunications Carriers (*except* Satellite) is the closest industry with a SBA small business size standard applicable to these services. The SBA small business size standard for this industry classifies a business as small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2017 show that there were 2,893 firms that operated in this industry for the entire year. Of this number, 2,837 firms employed fewer than 250 employees. Thus under the SBA size standard, the Commission estimates that a majority of licensees in this industry can be considered small.

17. The Commission's small business size standards with respect to WCS involve eligibility for bidding credits and installment payments in the auction of licenses for the various frequency bands included in WCS. When bidding credits are adopted for the auction of licenses in WCS frequency bands, such credits may be available to several types of small businesses based average gross revenues (small, very small and entrepreneur) pursuant to the competitive

bidding rules adopted in conjunction with the requirements for the auction and/or as identified in the designated entities section in Part 27 of the Commission's rules for the specific WCS frequency bands.

18. In frequency bands where licenses were subject to auction, the Commission notes that as a general matter, the number of winning bidders that qualify as small businesses at the close of an auction does not necessarily represent the number of small businesses currently in service. Further, the Commission does not generally track subsequent business size unless, in the context of assignments or transfers, unjust enrichment issues are implicated. Additionally, since the Commission does not collect data on the number of employees for licensees providing these services, at this time we are not able to estimate the number of licensees with active licenses that would qualify as small under the SBA's small business size standard.

19. *700 MHz Guard Band Licensees*. The 700 MHz Guard Band encompasses spectrum in 746-747/776-777 MHz and 762-764/792-794 MHz frequency bands. Wireless Telecommunications Carriers (*except* Satellite) is the closest industry with a SBA small business size standard applicable to licenses providing services in these bands. The SBA small business size standard for this industry classifies a business as small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2017 show that there were 2,893 firms that operated in this industry for the entire year. Of this number, 2,837 firms employed fewer than 250 employees. Thus under the SBA size standard, the Commission estimates that a majority of licensees in this industry can be considered small.

20. According to Commission data as of December 2021, there were approximately 224 active 700 MHz Guard Band licenses. The Commission's small business size standards with respect to 700 MHz Guard Band licensees involve eligibility for bidding credits and installment payments in the auction of licenses. For the auction of these licenses, the Commission defined a "small business" as an entity that, together with its affiliates and controlling principals, has average gross revenues not exceeding $40 million for the preceding three years, and a "very

small business" an entity that, together with its affiliates and controlling principals, has average gross revenues that are not more than $15 million for the preceding three years. Pursuant to these definitions, five winning bidders claiming one of the small business status classifications won 26 licenses, and one winning bidder claiming small business won two licenses. None of the winning bidders claiming a small business status classification in these 700 MHz Guard Band license auctions had an active license as of December 2021.

21. In frequency bands where licenses were subject to auction, the Commission notes that as a general matter, the number of winning bidders that qualify as small businesses at the close of an auction does not necessarily represent the number of small businesses currently in service. Further, the Commission does not generally track subsequent business size unless, in the context of assignments or transfers, unjust enrichment issues are implicated. Additionally, since the Commission does not collect data on the number of employees for licensees providing these services, at this time we are not able to estimate the number of licensees with active licenses that would qualify as small under the SBA's small business size standard.

22. *Lower 700 MHz Band Licenses*. The lower 700 MHz band encompasses spectrum in the 698-746 MHz frequency bands. Permissible operations in these bands include flexible fixed, mobile, and broadcast uses, including mobile and other digital new broadcast operation; fixed and mobile wireless commercial services (including FDD- and TDD-based services); as well as fixed and mobile wireless uses for private, internal radio needs, two-way interactive, cellular, and mobile television broadcasting services. Wireless Telecommunications Carriers (*except* Satellite) is the closest industry with a SBA small business size standard applicable to licenses providing services in these bands. The SBA small business size standard for this industry classifies a business as small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2017 show that there were 2,893 firms that operated in this industry for the entire year. Of this number, 2,837 firms employed fewer than 250 employees. Thus under the SBA

size standard, the Commission estimates that a majority of licensees in this industry can be considered small.

23. According to Commission data as of December 2021, there were approximately 2,824 active Lower 700 MHz Band licenses. The Commission's small business size standards with respect to Lower 700 MHz Band licensees involve eligibility for bidding credits and installment payments in the auction of licenses. For auctions of Lower 700 MHz Band licenses the Commission adopted criteria for three groups of small businesses. A very small business was defined as an entity that, together with its affiliates and controlling interests, has average annual gross revenues not exceeding $15 million for the preceding three years, a small business was defined as an entity that, together with its affiliates and controlling interests, has average gross revenues not exceeding $40 million for the preceding three years, and an entrepreneur was defined as an entity that, together with its affiliates and controlling interests, has average gross revenues not exceeding $3 million for the preceding three years. In auctions for Lower 700 MHz Band licenses seventy-two winning bidders claiming a small business classification won 329 licenses, twenty-six winning bidders claiming a small business classification won 214 licenses, and three winning bidders claiming a small business classification won all five auctioned licenses.

24. In frequency bands where licenses were subject to auction, the Commission notes that as a general matter, the number of winning bidders that qualify as small businesses at the close of an auction does not necessarily represent the number of small businesses currently in service. Further, the Commission does not generally track subsequent business size unless, in the context of assignments or transfers, unjust enrichment issues are implicated. Additionally, since the Commission does not collect data on the number of employees for licensees providing these services, at this time we are not able to estimate the number of licensees with active licenses that would qualify as small under the SBA's small business size standard.

25. *Upper 700 MHz Band Licenses*. The upper 700 MHz band encompasses spectrum in the 746-806 MHz bands. Upper 700 MHz D Block licenses are nationwide licenses associated with the 758-763 MHz and 788-793 MHz bands. Permissible operations in these bands include flexible fixed, mobile, and broadcast uses, including mobile and other digital new broadcast operation; fixed and mobile wireless commercial services (including FDD- and TDD-based services); as well as fixed and mobile wireless uses for private, internal radio needs, two-way interactive, cellular, and mobile television broadcasting services. Wireless Telecommunications Carriers (*except* Satellite) is the closest industry with a SBA small business size standard applicable to licenses providing services in these bands. The SBA small business size standard for this industry classifies a business as small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2017 show that there were 2,893 firms that operated in this industry for the entire year. Of that number, 2,837 firms employed fewer than 250 employees. Thus, under the SBA size standard, the Commission estimates that a majority of licensees in this industry can be considered small.

26. According to Commission data as of December 2021, there were approximately 152 active Upper 700 MHz Band licenses. The Commission's small business size standards with respect to Upper 700 MHz Band licensees involve eligibility for bidding credits and installment payments in the auction of licenses. For the auction of these licenses, the Commission defined a "small business" as an entity that, together with its affiliates and controlling principals, has average gross revenues not exceeding $40 million for the preceding three years, and a "very small business" an entity that, together with its affiliates and controlling principals, has average gross revenues that are not more than $15 million for the preceding three years. Pursuant to these definitions, three winning bidders claiming very small business status won five of the twelve available licenses.

27. In frequency bands where licenses were subject to auction, the Commission notes that as a general matter, the number of winning bidders that qualify as small businesses at the

close of an auction does not necessarily represent the number of small businesses currently in service. Further, the Commission does not generally track subsequent business size unless, in the context of assignments or transfers, unjust enrichment issues are implicated. Additionally, since the Commission does not collect data on the number of employees for licensees providing these services, at this time we are not able to estimate the number of licensees with active licenses that would qualify as small under the SBA's small business size standard.

28. *Advanced Wireless Services (AWS) - (1710–1755 MHz and 2110–2155 MHz bands (AWS-1); 1915–1920 MHz, 1995–2000 MHz, 2020–2025 MHz and 2175–2180 MHz bands (AWS-2); 2155–2175 MHz band (AWS-3); 2000-2020 MHz and 2180-2200 MHz (AWS-4)*. Spectrum is made available and licensed in these bands for the provision of various wireless communications services. Wireless Telecommunications Carriers (*except* Satellite) is the closest industry with a SBA small business size standard applicable to these services. The SBA small business size standard for this industry classifies a business as small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2017 show that there were 2,893 firms that operated in this industry for the entire year. Of this number, 2,837 firms employed fewer than 250 employees. Thus, under the SBA size standard, the Commission estimates that a majority of licensees in this industry can be considered small.

29. According to Commission data as December 2021, there were approximately 4,472 active AWS licenses. The Commission's small business size standards with respect to AWS involve eligibility for bidding credits and installment payments in the auction of licenses for these services. For the auction of AWS licenses, the Commission defined a "small business" as an entity with average annual gross revenues for the preceding three years not exceeding $40 million, and a "very small business" as an entity with average annual gross revenues for the preceding three years not exceeding $15 million. Pursuant to these definitions, 57 winning bidders claiming status as small or very small businesses won 215 of 1,087 licenses. In the most

recent auction of AWS licenses 15 of 37 bidders qualifying for status as small or very small businesses won licenses.

30. In frequency bands where licenses were subject to auction, the Commission notes that as a general matter, the number of winning bidders that qualify as small businesses at the close of an auction does not necessarily represent the number of small businesses currently in service. Further, the Commission does not generally track subsequent business size unless, in the context of assignments or transfers, unjust enrichment issues are implicated. Additionally, since the Commission does not collect data on the number of employees for licensees providing these services, at this time we are not able to estimate the number of licensees with active licenses that would qualify as small under the SBA's small business size standard.

31. *Broadband Radio Service and Educational Broadband Service*. Broadband Radio Service systems, previously referred to as Multipoint Distribution Service (MDS) and Multichannel Multipoint Distribution Service (MMDS) systems, and "wireless cable," transmit video programming to subscribers and provide two-way high speed data operations using the microwave frequencies of the Broadband Radio Service (BRS) and Educational Broadband Service (EBS) (previously referred to as the Instructional Television Fixed Service (ITFS)). Wireless cable operators that use spectrum in the BRS often supplemented with leased channels from the EBS, provide a competitive alternative to wired cable and other multichannel video programming distributors. Wireless cable programming to subscribers resembles cable television, but instead of coaxial cable, wireless cable uses microwave channels.

32. In light of the use of wireless frequencies by BRS and EBS services, the closest industry with a SBA small business size standard applicable to these services is Wireless Telecommunications Carriers (*except* Satellite). The SBA small business size standard for this industry classifies a business as small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2017 show that there were 2,893 firms that operated in this industry for the entire year. Of this number, 2,837 firms employed fewer than 250 employees. Thus under the SBA size

standard, the Commission estimates that a majority of licensees in this industry can be considered small.

33. According to Commission data as December 2021, there were approximately 5,869 active BRS and EBS licenses. The Commission's small business size standards with respect to BRS involves eligibility for bidding credits and installment payments in the auction of licenses for these services. For the auction of BRS licenses, the Commission adopted criteria for three groups of small businesses. A very small business is an entity that, together with its affiliates and controlling interests, has average annual gross revenues exceed $3 million and did not exceed $15 million for the preceding three years, a small business is an entity that, together with its affiliates and controlling interests, has average gross revenues exceed $15 million and did not exceed $40 million for the preceding three years, and an entrepreneur is an entity that, together with its affiliates and controlling interests, has average gross revenues not exceeding $3 million for the preceding three years. Of the ten winning bidders for BRS licenses, two bidders claiming the small business status won 4 licenses, one bidder claiming the very small business status won three licenses and two bidders claiming entrepreneur status won six licenses. One of the winning bidders claiming a small business status classification in the BRS license auction has an active licenses as of December 2021.

34. The Commission's small business size standards for EBS define a small business as an entity that, together with its affiliates, its controlling interests and the affiliates of its controlling interests, has average gross revenues that are not more than $55 million for the preceding five (5) years, and a very small business is an entity that, together with its affiliates, its controlling interests and the affiliates of its controlling interests, has average gross revenues that are not more than $20 million for the preceding five (5) years. In frequency bands where licenses were subject to auction, the Commission notes that as a general matter, the number of winning bidders that qualify as small businesses at the close of an auction does not necessarily represent the number of small businesses currently in service. Further, the Commission does not

generally track subsequent business size unless, in the context of assignments or transfers, unjust enrichment issues are implicated. Additionally, since the Commission does not collect data on the number of employees for licensees providing these services, at this time we are not able to estimate the number of licensees with active licenses that would qualify as small under the SBA's small business size standard.

35. *The Educational Broadcasting Services*. Cable-based educational broadcasting services fall under the broad category of the Wired Telecommunications Carriers industry. The Wired Telecommunications Carriers industry comprises establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired telecommunications networks. Transmission facilities may be based on a single technology or a combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including VoIP services; wired (cable) audio and video programming distribution; and wired broadband Internet services.

36. The SBA small business size standard for this industry classifies businesses having 1,500 or fewer employees as small. U.S. Census Bureau data for 2017 show that there were 3,054 firms in this industry that operated for the entire year. Of this total, 2,964 firms operated with fewer than 250 employees. Thus, under this size standard, the majority of firms in this industry can be considered small. Additionally, according to Commission data as of December 2021, there were 4,477 active EBS licenses. The Commission estimates that the majority of these licenses are held by non-profit educational institutions and school districts and are likely small entities.

37. *Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing*. This industry comprises establishments primarily engaged in manufacturing radio and television broadcast and wireless communications equipment. Examples of products

made by these establishments are: transmitting and receiving antennas, cable television equipment, GPS equipment, pagers, cellular phones, mobile communications equipment, and radio and television studio and broadcasting equipment. The SBA small business size standard for this industry classifies businesses having 1,250 employees or less as small. U.S. Census Bureau data for 2017 show that there were 656 firms in this industry that operated for the entire year. Of this number, 624 firms had fewer than 250 employees. Thus, under the SBA size standard, the majority of firms in this industry can be considered small.

38. *Software Publishers*. This industry comprises establishments primarily engaged in computer software publishing or publishing and reproduction. Establishments in this industry carry out operations necessary for producing and distributing computer software, such as designing, providing documentation, assisting in installation, and providing support services to software purchasers. These establishments may design, develop, and publish, or publish only. The SBA small business size standard for this industry classifies businesses having annual receipts of $41.5 million or less as small. U.S. Census Bureau data for 2017 indicate that 7,842 firms in this industry operated for the entire year. Of this number 7,226 firms had revenue of less than $25 million. Based on this data, we conclude that a majority of firms in this industry are small.

39. *Noncommercial Educational (NCE) and Public Broadcast Stations*. Noncommercial educational broadcast stations and public broadcast stations are television or radio broadcast stations which under the Commission's rules are eligible to be licensed by the Commission as a noncommercial educational radio or television broadcast station and are owned and operated by a public agency or nonprofit private foundation, corporation, or association; or are owned and operated by a municipality which transmits only noncommercial programs for education purposes.

40. The SBA small business size standards and U.S. Census Bureau data classify radio stations and television broadcasting separately and both categories may include both

noncommercial and commercial stations. The SBA small business size standard for both radio stations and television broadcasting classify firms having $41.5 million or less in annual receipts as small. For Radio Stations, U.S. Census Bureau data for 2017 show that 1,879 of the 2,963 firms that operated during that year had revenue of less than $25 million per year. For Television Broadcasting, U.S. Census Bureau data for 2017 show that 657 of the 744 firms that operated for the entire year had revenue of less than $25,000,000. While the U.S. Census Bureau data does not indicate the number of non-commercial stations, we estimate that under the applicable SBA size standard the majority of noncommercial educational broadcast stations and public broadcast stations are small entities.

41. According to Commission data as of March 31, 2022, there were 4,503 licensed noncommercial educational radio and television stations. In addition, the Commission estimates as of March 31, 2022, there were 384 licensed noncommercial educational (NCE) television stations, 383 Class A TV stations, 1,840 LPTV stations and 3,231 TV translator stations. The Commission does not compile and otherwise does not have access to financial information for these stations that permit it to determine how many stations qualify as small entities under the SBA small business size standards. However, given the nature of these services, we will presume that all noncommercial educational and public broadcast stations qualify as small entities under the above SBA small business size standards.

42. *Radio Stations*. This industry is comprised of "establishments primarily engaged in broadcasting aural programs by radio to the public." Programming may originate in their own studio, from an affiliated network, or from external sources. The SBA small business size standard for this industry classifies firms having $41.5 million or less in annual receipts as small. U.S. Census Bureau data for 2017 show that 2,963 firms operated in this industry during that year. Of this number, 1,879 firms operated with revenue of less than $25 million per year. Based on this data and the SBA's small business size standard, we estimate a majority of such entities are small entities.

43. The Commission estimates that as of March 31, 2022, there were 4,508 licensed commercial AM radio stations and 6,763 licensed commercial FM radio stations, for a combined total of 11,271 commercial radio stations. Of this total, 11,269 stations (or 99.98 %) had revenues of $41.5 million or less in 2021, according to Commission staff review of the BIA Kelsey Inc. Media Access Pro Database (BIA) on June 1, 2022, and therefore these licensees qualify as small entities under the SBA definition. In addition, the Commission estimates that as of March 31, 2022, there were 4,119 licensed noncommercial (NCE) FM radio stations, 2,049 low power FM (LPFM) stations, and 8,919 FM translators and boosters. The Commission however does not compile, and otherwise does not have access to financial information for these radio stations that would permit it to determine how many of these stations qualify as small entities under the SBA small business size standard. Nevertheless, given the SBA's large annual receipts threshold for this industry and the nature of these radio station licensees, we presume that all of these entities qualify as small entities under the above SBA small business size standard.

44. We note, however, that in assessing whether a business concern qualifies as "small" under the above definition, business (control) affiliations must be included. Our estimate, therefore, likely overstates the number of small entities that might be affected by our action, because the revenue figure on which it is based does not include or aggregate revenues from affiliated companies. In addition, another element of the definition of "small business" requires that an entity not be dominant in its field of operation. We are unable at this time to define or quantify the criteria that would establish whether a specific radio or television broadcast station is dominant in its field of operation. Accordingly, the estimate of small businesses to which the rules may apply does not exclude any radio or television station from the definition of a small business on this basis and is therefore possibly over-inclusive. An additional element of the definition of "small business" is that the entity must be independently owned and operated. Because it is difficult to assess these criteria in the context of media

entities, the estimate of small businesses to which the rules may apply does not exclude any radio or television station from the definition of a small business on this basis and similarly may be over-inclusive.

45. *FM Translator Stations and Low-Power FM Stations*. FM translators and Low Power FM Stations are classified in the industry for Radio Stations. The Radio Stations industry comprises establishments primarily engaged in broadcasting aural programs by radio to the public. Programming may originate in their own studio, from an affiliated network, or from external sources. The SBA small business size standard for this industry classifies firms having $41.5 million or less in annual receipts as small. U.S. Census Bureau data for 2017 show that 2,963 firms operated during that year. Of that number, 1,879 firms operated with revenue of less than $25 million per year. Therefore, based on the SBA's size standard we conclude that the majority of FM Translator stations and Low Power FM Stations are small. Additionally, according to Commission data, as of March 31, 2022, there were 8,919 FM Translator Stations and 2,049 Low Power FM licensed broadcast stations. The Commission however does not compile and otherwise does not have access to information on the revenue of these stations that would permit it to determine how many of the stations would qualify as small entities. For purposes of this regulatory flexibility analysis, we presume the majority of these stations are small entities.

46. *Television Broadcasting*. This industry is comprised of "establishments primarily engaged in broadcasting images together with sound." These establishments operate television broadcast studios and facilities for the programming and transmission of programs to the public. These establishments also produce or transmit visual programming to affiliated broadcast television stations, which in turn broadcast the programs to the public on a predetermined schedule. Programming may originate in their own studio, from an affiliated network, or from external sources. The SBA small business size standard for this industry classifies businesses having $41.5 million or less in annual receipts as small. 2017 U.S. Census Bureau data indicate

that 744 firms in this industry operated for the entire year. Of that number, 657 firms had revenue of less than $25,000,000. Based on this data we estimate that the majority of television broadcasters are small entities under the SBA small business size standard.

47. The Commission estimates that as of March 31, 2022, there were 1,373 licensed commercial television stations. Of this total, 1,280 stations (or 93.2%) had revenues of $41.5 million or less in 2021, according to Commission staff review of the BIA Kelsey Inc. Media Access Pro Television Database (BIA) on June 1, 2022, and therefore these licensees qualify as small entities under the SBA definition. In addition, the Commission estimates as of March 31, 2022, there were 384 licensed noncommercial educational (NCE) television stations, 383 Class A TV stations, 1,840 LPTV stations and 3,231 TV translator stations. The Commission however does not compile, and otherwise does not have access to financial information for these television broadcast stations that would permit it to determine how many of these stations qualify as small entities under the SBA small business size standard. Nevertheless, given the SBA's large annual receipts threshold for this industry and the nature of these television station licensees, we presume that all of these entities qualify as small entities under the above SBA small business size standard.

48. *Cable and Other Subscription Programming*. The U.S. Census Bureau defines this industry as establishments primarily engaged in operating studios and facilities for the broadcasting of programs on a subscription or fee basis. The broadcast programming is typically narrowcast in nature (e.g., limited format, such as news, sports, education, or youth-oriented). These establishments produce programming in their own facilities or acquire programming from external sources. The programming material is usually delivered to a third party, such as cable systems or direct-to-home satellite systems, for transmission to viewers. The SBA small business size standard for this industry classifies firms with annual receipts less than $41.5 million as small. Based on U.S. Census Bureau data for 2017, 378 firms operated in this industry during that year. Of that number, 149 firms operated with revenue of less than $25

million a year and 44 firms operated with revenue of $25 million or more. Based on this data, the Commission estimates that the majority of firms operating in this industry are small.

49. *Cable System Operators (Rate Regulation Standard)*. The Commission has developed its own small business size standard for the purpose of cable rate regulation. Under the Commission's rules, a "small cable company" is one serving 400,000 or fewer subscribers nationwide. Based on industry data, there are about 420 cable companies in the U.S. Of these, only seven have more than 400,000 subscribers. In addition, under the Commission's rules, a "small system" is a cable system serving 15,000 or fewer subscribers. Based on industry data, there are about 4,139 cable systems (headends) in the U.S. Of these, about 639 have more than 15,000 subscribers. Accordingly, the Commission estimates that the majority of cable companies and cable systems are small.

50. *Cable System Operators (Telecom Act Standard)*. The Communications Act of 1934, as amended, contains a size standard for a "small cable operator," which is "a cable operator that, directly or through an affiliate, serves in the aggregate fewer than one percent of all subscribers in the United States and is not affiliated with any entity or entities whose gross annual revenues in the aggregate exceed $250,000,000." For purposes of the Telecom Act Standard, the Commission determined that a cable system operator that serves fewer than 677,000 subscribers, either directly or through affiliates, will meet the definition of a small cable operator based on the cable subscriber count established in a 2001 Public Notice. Based on industry data, only six cable system operators have more than 677,000 subscribers. Accordingly, the Commission estimates that the majority of cable system operators are small under this size standard. We note however, that the Commission neither requests nor collects information on whether cable system operators are affiliated with entities whose gross annual revenues exceed $250 million. Therefore, we are unable at this time to estimate with greater precision the number of cable system operators that would qualify as small cable operators under the definition in the Communications Act.

51. *Satellite Telecommunications*. This industry comprises firms "primarily engaged in providing telecommunications services to other establishments in the telecommunications and broadcasting industries by forwarding and receiving communications signals via a system of satellites or reselling satellite telecommunications." Satellite telecommunications service providers include satellite and earth station operators. The SBA small business size standard for this industry classifies a business with $35 million or less in annual receipts as small. U.S. Census Bureau data for 2017 show that 275 firms in this industry operated for the entire year. Of this number, 242 firms had revenue of less than $25 million. Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 71 providers that reported they were engaged in the provision of satellite telecommunications services. Of these providers, the Commission estimates that approximately 48 providers have 1,500 or fewer employees. Consequently using the SBA's small business size standard, a little more than of these providers can be considered small entities.

52. *All Other Telecommunications*. This industry is comprised of establishments primarily engaged in providing specialized telecommunications services, such as satellite tracking, communications telemetry, and radar station operation. This industry also includes establishments primarily engaged in providing satellite terminal stations and associated facilities connected with one or more terrestrial systems and capable of transmitting telecommunications to, and receiving telecommunications from, satellite systems. Providers of Internet services (e.g. dial-up ISPs) or voice over Internet protocol (VoIP) services, via client-supplied telecommunications connections are also included in this industry. The SBA small business size standard for this industry classifies firms with annual receipts of $35 million or less as small. U.S. Census Bureau data for 2017 show that there were 1,079 firms in this industry that operated for the entire year. Of those firms, 1,039 had revenue of less than $25 million. Based on this data, the Commission estimates that the majority of "All Other Telecommunications" firms can be considered small.

53. *Direct Broadcast Satellite ("DBS") Service*. DBS service is a nationally distributed subscription service that delivers video and audio programming via satellite to a small parabolic "dish" antenna at the subscriber's location. DBS is included in the Wired Telecommunications Carriers industry which comprises establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired telecommunications networks. Transmission facilities may be based on a single technology or combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including VoIP services, wired (cable) audio and video programming distribution; and wired broadband internet services. By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry.

54. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small. U.S. Census Bureau data for 2017 show that 3,054 firms operated in this industry for the entire year. Of this number, 2,964 firms operated with fewer than 250 employees. Based on this data, the majority of firms in this industry can be considered small under the SBA small business size standard. According to Commission data however, only two entities provide DBS service - DIRECTV (owned by AT&T) and DISH Network, which require a great deal of capital for operation. DIRECTV and DISH Network both exceed the SBA size standard for classification as a small business. Therefore, we must conclude based on internally developed Commission data, in general DBS service is provided only by large firms.

D. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities

55. We expect the actions proposed in the *NPRM*, if adopted, will impose additional reporting, recordkeeping and/or other compliance obligations on small as well as other entities who are EAS Participants and Participating CMS Providers. More specifically, if adopted, EAS Participants and Participating CMS Providers would be required to annually certify to creating, updating, and implementing a cybersecurity risk management plan to ensure the confidentiality, integrity, and availability of their respective alerting systems. The cybersecurity risk management plan must contain among other things, a description of how organizational resources are employed to ensure the confidentiality, integrity, and availability of the alerting system. Further, any incident involving the unauthorized access to EAS equipment, communications systems, or services, regardless of whether the event resulted in the transmission of a false alert would require EAS Participants to report the unauthorized access to the Commission within 72 hours of when the EAS Participant knew or should have known that an incident has occurred. The Commission also seeks comment on whether and how to strengthen the operational readiness of the EAS.

56. In assessing the cost of compliance with our proposed rule to create a cybersecurity risk management plan, we estimate the cost for each small EAS Participant and each Participating CMS Providers to be approximately $820. These costs are based on 10 hours of labor at $82 an hour and apply to all EAS Participants and Participating CMS Providers not just small entities. We anticipate however, that many small EAS Participants and Participating CMS Providers will not require 10 hours to develop or update a cybersecurity risk management plan tailored to the size of their organization. The cost for reporting an unauthorized access incident we believe would be similar to the cost of reporting a false alert, which the Commission has estimated to have a total cost of $11,600 per year across 290 EAS Participants. This total cost when apportioned to each EAS Participant comes out to approximately $40 per EAS Participant.

57. We estimate a $9.2 million one-time cost for all Participating CMS Providers, not just small providers, to update the WEA standards and software necessary to comply with our proposed rule that Participating CMS Providers transmit sufficient authentication information to allow mobile devices to present WEA alerts only if they come from valid base stations. This figure consists of approximately a $500,000 cost to update applicable WEA standards and approximately an $8.7 million cost to update applicable software. We quantify the cost of modifying standards as the annual compensation for 30 network engineers compensated at the national average for their field ($85,816/year; $41.26/hour), plus annual benefits ($26,775/year; 12.87/hour) working for the amount of time that it takes to develop a standard (one hour every other week for one year, 26 hours) for 12 distinct standards. We quantify the cost of modifying software as the annual compensation for a software engineer compensated at the national average for their field ($86,998/year), plus annual benefits ($27,143/year) working for the amount of time that it takes to develop software (one year) at each of the 76 CMS Providers that participate in WEA.

58. At this time the Commission cannot quantify the cost of compliance for small entities to comply with the other proposals or approaches on which it seeks comment in the *NPRM*. We believe that the modifications to improve and enhance the security of the EAS that we discuss in the *NPRM* are the most efficient and least burdensome approach and do not believe small entities will have to hire professionals to meet the requirements discussed in the *NPRM,* if adopted. To help the Commission more fully evaluate the cost of compliance for small entities should our proposals be adopted, in the *NPRM*, we request comments on the cost implications of our proposals and ask whether there are more efficient and less burdensome alternatives (including cost estimates) for the Commission to consider. We expect the information we receive in comments including cost and benefit analyses, will help the Commission identify and evaluate relevant matters for small entities, including compliance costs and other burdens that may result from the proposals and inquiries we make in the *NPRM*.

E. Steps Taken to Minimize the Significant Economic Impact on Small Entities, and Significant Alternatives Considered

59. The RFA requires an agency to describe any significant, specifically small business alternatives that it has considered in reaching its proposed approach, which may include (among others) the following four alternatives: (1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance or reporting requirements under the rule for such small entities; (3) the use of performance, rather than design, standards; and (4) and exemption from coverage of the rule, or any part thereof, for such small entities.

60. The Commission has taken steps to minimize the impact of the proposals in the *NPRM* as a general matter, and specifically targeting small entities, has sought comment on the extent to which we can limit the overall economic impact of these proposed requirements if we provide increased flexibility for businesses classified as small under the SBA small business size standard. Below we discuss actions taken and alternatives considered by the Commission for the rules proposed promoting the operational readiness of EAS equipment, improving awareness of unauthorized access to EAS equipment, communications systems, and services, and requiring the development, implementation, and certification of a cybersecurity risk management plan.

61. To further the Commission's objectives to promote EAS equipment operational readiness, in the *NPRM* we seek comment on whether to require EAS Participants to repair EAS equipment with prompt and reasonable diligence, on whether the EAS Participants should notify the Commission of the status of their repairs, and, if so, on the timing, content, and means of that notification.

62. We seek comment on whether a compliance timeframe of 30 days from publication in the *Federal Register* of notice that the Office of Management and Budget (OMB) has completed its review of the modified information collection to improve the Commission's

visibility into the repair or replacement of non-operational EAS equipment would not impose a burden on small entities. Small and other EAS Participants currently make entries in their broadcast station logs and cable system records showing the date and time equipment was removed and restored to service, and therefore already have processes and procedures in place to record information about the operational status of their EAS equipment in station logs that could be utilized for the proposed notification requirement. In the event that the Commission were to alternatively require this notification to be provided through NORS, the requirement would become effective within 30 days from publication in the *Federal Register* of notice that the OMB has approved the modified information collection or upon publication in the *Federal Register* of a Public Notice announcing that NORS is technically capable of receiving such notifications, whichever is later. Similarly, this requirement should not impose a burden on small entities for the reason stated above and since EAS Participants are already likely to be using NORS.

63. Our approach to improving awareness of unauthorized access to EAS equipment, communications systems, and services relies on our belief that significant public safety benefits will accrue if EAS Participants were required to provide the Commission with notification that their EAS equipment, communications systems, and services have been accessed without authorization, even in the absence of a subsequent transmission of a false alert. The reporting requirement we proposed in the *NPRM* requiring EAS Participants to provide notification to the Commission via NORS within 72 hours of when an EAS Participant knew or should have known that an incident has occurred should result in low marginal costs for small and other EAS participants since our requirement parallels the reporting obligations EAS Participants may have to other government agencies that require critical infrastructure sector entities to report cyber incidents. This would allow the requirement to be satisfied by reporting substantially similar information to another federal agency in a similar timeframe. We believe the cost to report unauthorized access is comparable to the cost of reporting false alerts which further supports our belief that these costs will be relatively low for small and other EAS Participants. In the *NPRM*

we have requested comments and cost and benefit analyses on our proposal and beliefs. In addition, we have requested alternative proposals (accompanied by cost analyses) for unauthorized access reporting requirements that would be less costly for small and other EAS Participants while producing similar or greater benefits.

64. The requirement for EAS Participants to report any incident of unauthorized access of its EAS equipment, communications systems, or services would be effective 60 days from publication in the *Federal Register* of notice that the OMB has approved the modified information collection. Since we consider the requirement to report unauthorized access similar to the Commission's false alert reporting requirement, there are likely to be compliance synergies for small and other EAS Participants, and less of a burden than there would be in the absence of the similarity. We therefore seek comment in the *NPRM* on whether an EAS Participant's process for ascertaining whether an incident of unauthorized access of its EAS equipment, communications systems, or services has occurred and reporting it to the Commission entails a level of effort comparable to compliance with the Commission's false alert reporting requirement.

65. To further explore the impact of the cybersecurity risk management plan requirement proposed in the *NPRM* which requires small and other EAS Participants and Participating CMS Providers to create, implement, and annually update a cybersecurity risk management plan and submit an annual certification attesting to compliance with requirement, Commission seeks comment on steps that it could take to limit various burdens. In particular, the Commission requests comment on whether the steps that it describes for EAS Participants and Participating CMS Providers to submit their risk management plans are the most efficient way to implement a certification requirement. In the *NPRM*, we propose to afford each EAS Participant and Participating CMS Provider the flexibility to include content in its plan that is tailored to its organization, provided that the plan demonstrates how the EAS Participant or Participating CMS Provider identifies the cyber risks that they face, the controls they use to

mitigate those risks, and how they ensure that these controls are applied effectively to their operations.

66. The Commission also proposes to require that each plan include security controls sufficient to ensure the confidentiality, integrity, and availability (CIA) of the EAS. While we believe there are numerous methods to satisfy this aspect of the requirement, we have proposed to allow the requirement to be satisfied by providing evidence of the successful implementation of an established set of cybersecurity best practices, such as applicable Center for Internet Security (CIS) Critical Security Controls or the Cybersecurity & Infrastructure Security Agency (CISA) Cybersecurity Baseline. We believe adopting this flexible approach will allow EAS Participants and Participating CMS Providers to develop a plan that is appropriate for their organization's size and available resources, while still ensuring that the plan results in ongoing and material improvements in EAS and WEA security. The Commission anticipates that this flexibility will reduce the costs imposed on small business EAS Participants and Participating CMS Providers, which will have different cybersecurity needs than larger EAS Participants and Participating CMS Providers, respectively. We do note, however, that to ensure that every EAS Participant implements a baseline of security controls, the Commission proposes to require that each plan include certain security measures: changing default passwords prior to operation, installing security updates in a timely manner, securing equipment behind properly configured firewalls or using other segmentation practices, requiring multifactor authentication where applicable, addressing the replacement of end-of-life equipment, and wiping, clearing, or encrypting user information before disposing of old devices.

67. The Commission proposes to require compliance with the requirement to implement a cybersecurity risk management plan and certification within twelve months of the publication in the *Federal Register* of notice that the OMB has approved the modified information collection. We recognize that larger EAS Participants are likely to already have cybersecurity risk management plans in place. We ask whether we should allow small entities a

two-year timeframe to implement this requirement. The two-year timeframe should provide sufficient time for small EAS Participants and small Participating CMS Providers that do not already have a risk management plan in place to create one. The timeframe would also be sufficient to prepare their organizations to manage security and privacy risks, categorize their systems and the information being processed, stored, and transmitted, and select controls to protect their systems. Further, a two-year timeframe would provide time for these entities to implement the security controls that the plan describes, assess whether the controls are in place, operating as intended, and producing the desired results, appoint a senior official to authorize the system, and develop mechanisms to continuously monitor control implementation and risks to the system.

68. In the *NPRM*, the Commission identifies alternative approaches on several matters that might minimize the economic impact for small entities. For example, the Commission requests alternatives to providing a second notification to the Commission once repairs of EAS equipment have been completed, and the EAS Participant's EAS systems have been tested and determined to once again be fully functional. The Commission seeks comment on potential alternatives to, and additional aspects of, the discussed approach, as well as their accompanying costs and benefits. The Commission recommends that EAS Participants file the required notifications regarding EAS equipment failures and repairs in the NORS database, but requests comment on other means EAS Participants could use to submit the notifications such as via email to a designated e-mail address.

69. The Commission expects to more fully consider the economic impact and alternatives for small entities following the review of comments filed in response to the *NPRM,* including costs and benefits analyses. Having data on the costs and economic impacts of proposals and approaches will allow the Commission to better evaluate options and alternatives for minimization of any significant economic impact on small entities as a result of the proposals and approaches raised in the *NPRM*. The Commission's evaluation of this information will

shape the final alternatives it considers to minimize any significant economic impact that may occur on small entities, the final conclusions it reaches, and any final rules it promulgates in this proceeding.

F. Federal Rules that May Duplicate, Overlap, or Conflict with the Proposed Rules

70. None.

II. Notice of Proposed Rulemaking

A. Promoting the Operational Readiness of EAS Equipment

71. We observe that, according to the Bureau's last nationwide EAS test report, an appreciable number of EAS Participants were unable to participate in testing due to equipment failure –despite advance notice that such test was to take place – suggesting that equipment failures are not addressed by EAS Participants as swiftly as reasonably possible and that more needs to be done to improve EAS operational readiness. Today, EAS Participants may continue operations for a period of 60 days despite having defective equipment that preclude their participation in EAS. We seek comment on whether this approach is effective at ensuring the operational readiness of EAS. How frequently does EAS equipment encounter defects that prevent it from receiving or retransmitting alerts? What are the most common types of defects that are experienced? What steps are necessary to repair these defects, and how often do they typically take to repair? Do EAS Participants take prompt steps to repair their EAS equipment, or do they typically take several days or weeks before seeking repairs? Do other EAS stakeholders, such as alert originators, have concerns about equipment failures preventing the transmission of emergency alerts to the public? We encourage commenters to highlight any specific incidences in which an EAS equipment defect prevented members of the public from being alerted to an emergency.

72. We seek comment on how to better promote the operational readiness of EAS equipment. For example, instead of requiring repairs within 60 days, would it serve the public

interest to require EAS Participants to conduct repairs promptly and with reasonable diligence? Are all EAS Participants already doing so? If so, what are the reasons why some EAS Participants are not able to conduct repairs promptly and diligently? What factors should we consider when determining whether repairs are made promptly and with reasonable diligence? What barriers prevent equipment from being repaired promptly and what steps can we take to remove those barriers?

73. Would it improve EAS operational readiness and public safety in general to increase the situational awareness of the Commission, alert originators, and others about the occurrence of equipment defects that might prevent alerts from reaching the public? For example, would such an approach allow us to better enforce our operational readiness rules and identify persistent technical problems, and make contingency plans for alert delivery? If so, should we adopt an EAS equipment defect notification requirement? For example, should we require EAS Participants to report EAS equipment defects and submit a follow-up notification when the equipment is repaired? Within what timeframe should they perform that notification to ensure that stakeholders are aware of possible impacts on EAS (e.g. 24 hours)? What content should the notification contain? For example, should notifications include the same information that is already included in requests for additional repair time that are required sent to the Regional Director of the FCC field office for the area that the EAS Participant serves? We seek comment on how, if at all, the Commission should share information to promote situational awareness among relevant stakeholders, such as alert originators State Emergency Communications Committees. We also seek comment on whether to treat this information as confidential and, if so, how to protect it. Are there other steps that we should take to better ensure that EAS is ready and available when it is needed?

74. We seek comment on any measures that the Commission could take to reduce burdens on EAS Participants if it were to take further steps to promote the operational readiness of EAS equipment. Should we remove the requirement under § 11.35(b) that EAS Participants

make entries in their own broadcast station log and cable system records showing the date and time the equipment was removed and restored to service? Would the elimination of the "60 day" rule in favor of a prompt repair rule reduce certain burdens on EAS Participants? We seek comments on the costs of any approaches to improving EAS operational readiness that commenters propose that we consider. In doing so, commenters should offer specific cost estimates where possible. For example, we seek comment on whether it would be reasonable to estimate that EAS Participants would transmit a maximum of 2,000 EAS equipment defect notifications annually under the approach discussed above, as 565 EAS Participants reported their equipment was defective during the 2021 Nationwide EAS Test? Would it be reasonable to estimate that 2,000 annual notifications would require one hour of labor each from a General and Operations Manager who is compensated at $82 per hour, resulting in an overall cost of $164,000? We seek similarly detailed analysis on potential alternatives to improve EAS operational readiness.

B. Improving Awareness of Unauthorized Access to EAS Equipment

75. Section 11.45(b) of the Commission's rules requires that an EAS Participant notify the Commission by e-mail within 24 hours of its discovery that it has transmitted or otherwise sent a false alert to the public, including details concerning the event. We believe that it would be in the public interest to strengthen this rule in view of the increasing threats that cyber attacks pose to EAS networks and equipment. Accordingly, we propose to revise this rule to further require that an EAS Participant report any incident of unauthorized access of its EAS equipment (i.e., regardless of whether that compromise has resulted in the transmission of a false alert), to the Commission via NORS within 72 hours of when it knew or should have known that an incident has occurred and provide details concerning the incident. We seek comment on this proposal.

76. We observe that protecting EAS equipment alone is unlikely to be sufficient to protect the EAS from a cyber attack. Even without directly accessing an EAS Participant's EAS

equipment, a bad actor could send a false alert or prevent a legitimate alert with lifesaving information from reaching the public by gaining unauthorized access to EAS Participants' communications systems and services. For this reason, we also propose to require that an EAS Participant report any incident of unauthorized access to any aspects of an EAS Participant's communications systems and services that potentially could affect their provision of EAS. This would include infrastructure that serves to prevent unauthorized access to EAS equipment, including firewalls and Virtual Private Networks. We seek comment on this proposal and on any suitable alternatives.

77. We believe the proposed rule is justified in light of the instances of false EAS alerts in recent years, caused by compromised EAS equipment being used to transmit a false message. As recounted above, we are aware of several situations in the past decade in which bad actors were either capable of obtaining, or actually obtained unauthorized access to EAS equipment. We seek comment on these views. Are there any other past or present security incidents involving EAS about which the Commission should be aware? Does unauthorized access to EAS equipment provide bad actors with the ability to disrupt EAS Participants' regularly scheduled programming, which has the potential to inflict financial harm in relation to their advertisers and reputational harm with their audiences? Are there any other kinds of harms resulting from unauthorized access to EAS equipment that the Commission should consider?

78. We believe significant public safety benefits would accrue if EAS Participants were required to provide the Commission with notification that their EAS equipment, communications systems, or services have been accessed without authorization, even in the absence of a subsequent transmission of a false alert. This view is based on our observation that, after a system is compromised, many attackers will position themselves to attack connected systems in several different ways. For example, we have observed that it is characteristic of some cyber attacks that an attacker will start by compromising one device and then, prior to launching a specific attack, spend time and effort to identify and compromise other devices in the

network, potentially using the initially comprised device as an access point to other devices. The Commission could use the proposed notifications to work with providers and other government agencies to resolve an equipment compromise before the compromise is actually exploited to cause false EAS transmissions in at least some instances. We further believe that the Commission could leverage information on the frequency and nature of equipment compromise to better understand the prevalence and trends associated such attacks across the nation. The Commission and its government partners would thus be better apprised of the risks posed to EAS and in a position to use this information to inform further measures that might be necessary to secure EAS.

79. We seek comment on these views, including detailed information as to the associated costs and benefits of the proposed approach. For example, what would be a reasonable estimate of the financial harm that such a cyber attack would inflict upon an EAS Participant, and how should such estimates be calculated? We believe the cost of reporting an unauthorized access incident would tend to be similar to the cost of reporting a false alert, which the Commission has estimated to have a total cost of $11,600 per year across all EAS Participants. We seek comment on that estimate. Are EAS Participants already conducting investigations and gathering information about suspected incidents of unauthorized access to EAS equipment, communications systems, and services? Are there less costly alternatives to an unauthorized access reporting requirement that would achieve similar or greater benefits? We believe that the marginal costs of an unauthorized access reporting requirement are likely to be low, as the requirement parallels the requirements of an upcoming CISA rulemaking. Specifically, CISA is required by the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) to adopt rules requiring critical infrastructure sector entities to report cyber incidents, but allows the requirement to be satisfied by reporting substantially similar information to another federal agency in a similar timeframe. We seek comment on that belief.

80. We propose to define "unauthorized access" to EAS equipment, communications systems, and services for the purposes of today's proposal to refer to any incident involving either remote or local access to EAS equipment, communications systems, or services by an individual or other entity that either does not have permission to access the equipment or exceeds their authorized access. We seek comment on this definition. For example, does this proposed definition mirror the methods that have been, and are likely to be, used by cyber-attackers to infiltrate EAS? We seek comment on whether it is appropriate to require that EAS Participants provide notification to the Commission within 72 hours of when they knew or should have known that an incident has occurred. Is this time frame appropriate or would it, for example, put undue pressure on EAS Participants at a critical time when they may be attempting to fully diagnose and resolve the compromise to their systems? On the other hand, is this time frame too slow to provide the Commission and government partners with timely notice of an incident? For example, consistent with the NORS reporting deadlines for interconnected VoIP outages, should the Commission be notified within 24 hours of a reasonable belief that an incident has occurred? In the alternative, should we require EAS Participants to provide notification to the Commission within 72 hours of "its reasonable belief that an incident has occurred," consistent with the approach to cyber incident reporting outlined by CIRCIA? Or, would this approach create disincentives for a provider to monitor the security of its own network? Would any alternative approach be more effective? Similar to what is contemplated by CIRCIA, should EAS Participants be required to submit updates to the Commission if substantial new or different information becomes available, until the date that the Commission is notified that the incident has concluded and been fully mitigated and resolved? Is the overall approach we propose today consistent with the incident reporting requirements of other federal and state government agencies, and if not, how should our proposal be harmonized to be more consistent with those requirements?

81. We seek comment on the kinds of information that should be included in reports of unauthorized access. We propose that reports include, to the extent it is applicable and available at the time of reporting, the date range of the incident, a description of the unauthorized access, the impact to the EAS Participant's EAS operational readiness, a description of the vulnerabilities exploited and the techniques used to access the device, identifying information for each actor responsible for the incident, and contact information for the EAS Participant. We believe this information is necessary to understand the unauthorized access incident, resolve it before the compromise is actually exploited to send a false alert, and harmonize our requirements with those of other federal agencies. We seek comment on the proposed content of these reports and whether it should be modified. We propose that the contents of these reports be treated as presumptively confidential and only shared on a confidential basis with other Federal agencies and state government agencies that agree to protect them to the same extent and in the same manner as the Commission would and, to the extent that the policies or regulations of those agencies are stricter, to the same extent and in the same manner as they would if they had collected the information themselves. We also propose to allow disclosure by the Commission, or by parties with whom the Commission has shared the notifications, of anonymized information about breaches that might be useful for industry, security researchers, policymakers, and the general public. We seek comment on this approach to cyber incident information sharing.

82. We seek comment on how these reports should be submitted to the Commission. Should they be submitted to the FCC Operation Center by e-mail, in similar fashion to the false alert reports that EAS Participants are already required to file with the Commission? Should these reports be submitted in NORS to better capture the required contents in clearly defined fields and more easily facilitate sharing with federal partners? Or should we develop a new electronic database to collect the content of the reports? Are there other approaches we should consider? What are the costs and benefits associated with each approach? We seek comment on

whether Participating CMS Providers should also be required to report incidents of unauthorized access to their WEA systems, or services. Similar to EAS, we believe that such a requirement would allow the Commission and its government partners to better identify and evaluate risks posed to EAS and inform further measures that might be necessary to secure WEA. Should reports be required in the same timeframe and with the same content as proposed for EAS? Are there any differences between EAS and WEA that would warrant differing unauthorized access reporting requirements for WEA? If so, what are those differences and how should the requirements be modified to reflect them?

C. Protecting the Nation's Alerting Systems through the Development, Implementation, and Certification of a Cybersecurity Risk Management Plan

1. EAS Security

83. As discussed above, the EAS has faced cybersecurity risks for more than a decade, with PSHSB regularly advising EAS Participants to follow cybersecurity best practices and take other steps to improve their cybersecurity posture. Despite these admonitions, however, we have not observed meaningful security improvements. For example, PSHSB has frequently advised EAS Participants to update their EAS software to ensure that they have installed the most recent security patches, including one such round of outreach in 2020 after the discovery that certain EAS equipment was potentially vulnerable to IP-based attacks. However, in filings related to the Nationwide EAS Test in August 2021, the Bureau observed that more than 5,000 EAS Participants were using outdated software or using equipment that no longer supported regular software updates. In light of these failures, we believe the Commission should take action to ensure the security of EAS.

84. We propose to require EAS Participants to submit an annual certification attesting that they have created, updated, and implemented a cybersecurity risk management plan. The cybersecurity risk management plan would describe how the EAS Participant employs their

organizational resources and processes to ensure the confidentiality, integrity, and availability of the EAS. The plan must discuss how the EAS Participant identifies the cyber risks that they face, the controls they use to mitigate those risks, and how they ensure that these controls are applied effectively to their operations. We believe that this certification requirement would improve the overall security of EAS by ensuring that EAS Participants are regularly taking steps to address security threats as part of their organization's day-to-day strategic and operational planning. We also believe the creation and implementation of cybersecurity risk management plans would help to ensure EAS operational readiness and eliminate false alerts, which divert public safety and other government resources from other important activities, impose costs on EAS Participants that have to deal with many of the consequences and, ultimately, desensitize the public to legitimate alerts. We seek comment on this proposal. Do stakeholders agree this proposal would improve the security of the EAS? Are there other benefits that may accrue from the creation and implementation of cybersecurity risk management plans by EAS Participants? Is an annual certification the right frequency with which to file certifications, or are there circumstances where more (or less) frequent filings might be necessary?

85. We propose to afford each EAS Participant flexibility to structure its plan in a manner that is tailored to its organization, provided that the plan demonstrate that the EAS Participant is taking affirmative steps to analyze security risks and improve its security posture. While we believe there are many ways for EAS Participants to satisfy this requirement, we propose that EAS Participants can successfully demonstrate that they have satisfied this requirement by structuring their plans to follow an established risk management framework, such as the National Institute of Standards and Technology (NIST) Risk Management Framework or the NIST Cybersecurity Framework. We believe this flexible approach would allow EAS Participants to develop a plan that is appropriate for their organization's size and available resources, while still ensuring that the plan results in ongoing and material improvements in EAS security. We also anticipate that this requirement would reduce the costs imposed on smaller

EAS Participants, which may have different cybersecurity needs than larger EAS Participants. We seek comment on this proposal. Alternatively, should we require EAS Participants to structure their plans to follow the NIST Risk Management Framework or the NIST Cybersecurity Framework? If so, should we require EAS Participants to follow the current version of each framework (i.e., Risk Management Framework for Information Systems and Organizations, NIST Special Publication 800-37, Revision 2; NIST Cybersecurity Framework V1.1)? If we take this approach, we anticipate that NIST may one day release updated versions of these frameworks, and we would then expect to seek notice and comment on whether we should require EAS Participants to follow the updated versions. We seek comment on this approach.

86. We propose that each cybersecurity risk management framework include security controls sufficient to ensure the confidentiality, integrity, and availability (CIA) of the EAS. We expect that reasonable security measures will include measures that are commonly the subject of best practices. While we believe there are potentially many ways for EAS Participants to satisfy this aspect of the requirement, we propose that EAS Participants will have satisfied it if they demonstrate they have successfully implemented an established set of cybersecurity best practices, such as applicable CIS Critical Security Controls or the CISA Cybersecurity Baseline. To ensure that every EAS Participant implements a baseline of security controls, however, we propose to require that each plan include security measures that address changing default passwords prior to operation, installing security updates in a timely manner, securing equipment behind properly configured firewalls or using other segmentation practices, requiring multifactor authentication where applicable, addressing the replacement of end-of-life equipment, and wiping, clearing, or encrypting user information before disposing of old devices. We expect that compliant cybersecurity risk management plans will not be limited to only these specific measures, as plans will vary based on individual providers' needs and circumstances and will need regular updates to keep up with an evolving threat environment. We seek comment on

these proposed rules. Are there other specific security measures that we should require EAS Participants to implement? For example, should we require EAS Participants to conduct network security audits or vulnerability assessments to identify potential security vulnerabilities? If so, how often should they be conducted? Should we require EAS Participants to report to the Commission when their network audits, network vulnerability assessments, or penetration testing reports reveal critical vulnerabilities? If so, how should we define a "critical vulnerability" for this purpose? Should we require EAS Participants to implement Incident Response Plans that describe how the procedures that EAS Participants would follow when respond to an ongoing cybersecurity incident? Should we require EAS Participants to conduct cybersecurity training for their employees or contractors and if so, what should the contents of that training be? What kinds of security measures have EAS Participants already implemented to protect the EAS, and how effective are they at mitigating cybersecurity risks? Should we require EAS Participants to keep records that demonstrate how they have implemented each of the baseline security controls? If so, what specific types of information should the records include and for how long should they be kept? Have EAS Participants identified unsuccessful attempts to access their systems, and if so, what specific security measures best thwarted those attempts?

87. Does this approach strike the appropriate balance between improving EAS security, complementing EAS Participants' existing cybersecurity activities, and reducing burdens on small EAS Participants? If not, how should this requirement be modified to achieve that balance? We seek comment on whether this approach grants too much flexibility and will not result in improvements to EAS security. We also seek comment on alternative approaches that would be effective at improving EAS security. For example, should we require EAS Participants to address a specified list of cybersecurity subject matters in their risk management plans? Instead of requiring the use of a risk management plan, should we require EAS Participants to take specific steps to secure their EAS equipment? If so, could such a requirement be drafted in a way to encourage EAS Participants to continually examine and

improve their cybersecurity posture, rather than merely check items off a list? Is our proposed certification requirement too burdensome on small EAS Participants? If so, what would be a more cost-effective way to promote EAS security for small EAS Participants?

88. We observe that protecting EAS equipment alone is unlikely to be sufficient to protect the EAS from a cyber attack. In addition to the risk of a bad actor sending a false alert, a bad actor could attack other elements of an EAS Participant's systems or service as a way to prevent a legitimate alert with lifesaving information from reaching the public. For this reason, we propose to require that the cybersecurity risk management plan address not only the security of EAS equipment, but also the security of all aspects of an EAS Participant's communications systems and services that potentially could affect their provision of EAS. We seek comment on this requirement. Are there alternative requirements that we should consider to ensure that bad actors cannot prevent the transmission of legitimate alerts (or engage in the transmission of false ones)?

89. We seek comment on whether there are industry groups, cybersecurity organizations, or other organizations that may be positioned to help EAS Participants create, implement, and maintain their cybersecurity risk management plan. What kinds of resources do these organizations offer, and how can EAS Participants make use of them? For example, are there organizations that offer, or that would be able to begin offering, authoritative sources of cybersecurity information and expertise? Are there organizations that can support EAS Participants by offering cybersecurity training, risk management plan templates, or otherwise promote the cybersecurity? If so, to what extent can these organizations help reduce the burdens related to the proposed certification requirement and make EAS more secure?

90. We propose that EAS Participants certify to creating, annually updating, and implementing a cybersecurity risk management plan by checking a box as part of its annual filing of EAS Test Reporting System Form One. We seek comment on whether this is the most efficient way to implement a certification requirement for EAS Participants. If not, how should

the certification be implemented? While the Commission does not intend to review each individual plan for sufficiency, we propose that the cybersecurity risk management plan be made available to the Commission upon request so that the Commission may review a specific plan as needed or proactively review a sample of EAS Participants' plans to ensure that they are sufficient to ensure the confidentiality, integrity, and availability of the EAS. In such circumstances, cybersecurity risk management plans would be treated as presumptively confidential. We propose to delegate to the Bureau the authority to request review of such cybersecurity risk management plans and to evaluate them for sufficiency. We seek comment on this approach to evaluating plans. For how long we should require EAS Participants to retain prior versions of their cybersecurity risk management plans to enable the Bureau's review?

91. We propose that the filing of, and subsequent compliance with, a cybersecurity risk management plan would not serve as a safe harbor or excuse or any other diminishment of responsibility for negligent security practices. We believe that allowing the filing of and compliance with a plan to have such an effect could create a perverse incentive. EAS Participants must remain constantly vigilant in preventing intrusions and can only satisfy that responsibility by acting reasonably in all circumstances. Any negligence in protecting the confidentially, integrity, and availability of EAS that results in transmission of false alerts or non-transmission of valid EAS messages would establish a violation of that duty, regardless of the content of the plan. Furthermore, we propose that an EAS Participant's failure to sufficiently develop or implement their plan, would be treated as a violation of the proposed rules. We seek comment on the criteria or indicia that we should consider when determining whether a plan is insufficient to mitigate cyber risk. We also seek comment on any measures that the Commission should take to verify whether EAS Participants have implemented of their plans.

92. We believe that the benefits of this proposal outweigh the costs. While we believe that it is impossible to quantify the precise dollar value of improvements to the public's safety, life, and health, as a general matter, we nonetheless believe that very substantial public

safety benefits will result from the rules we propose today: EAS will be better able to ensure that real alerts with lifesaving information are successfully delivered to the public and false alerts are prevented in order to preserve public trust and better ensure that the public takes appropriate action during real emergencies. As a consequence, we anticipate that the rule changes we adopt today will yield substantial life-saving benefits. Independent of that analysis, the Commission has previously found that "a foreign adversary's access to American communications networks could result in hostile actions to disrupt and surveil our communications networks, impacting our nation's economy generally and online commerce specifically, and result in the breach of confidential data." Consistent with the Commission's past analysis, our national gross domestic product was nearly $23 trillion last year, adjusting for inflation. Accordingly, if creating and implementing a cybersecurity risk management plan prevents even a 0.005% disruption to our economy, we believe our proposed requirement would generate $1.15 billion in benefits. Likewise, the digital economy accounted for $3.31 trillion of our economy in 2020, and so we believe preventing a disruption of even 0.05% would produce benefits of $1.66 billion. As a check on our analysis, consider the impact of existing malicious cyber activity on the U.S. economy: $57 billion to $109 billion in 2016. Given the incentives and documented actions of hostile nation-state actors, reducing this activity (or preventing an expansion of such damage) by even 1% would produce benefits of $0.57 billion to $1.09 billion. Given this analysis, we believe the benefits of our rule to the American economy, commerce, and consumers are likely to significantly and substantially outweigh the costs of the proposed certification requirement. We seek comment on this analysis. Is there a more appropriate way to quantify these benefits? Are there any additional ways in which the proposed rules would benefit the public that the Commission should consider?

93. We estimate that the overall cost of our proposed cybersecurity risk management plan requirement will be approximately $21 million. We believe that EAS Participants will, on average, require 10 hours annually to initially draft a plan and then update the plan and submit

their certification annually. When developing this average we anticipate that many large EAS Participants already have cybersecurity risk management plans and will incur only de minimis costs to comply with this requirement. We also anticipate that many small EAS Participants will require less than 10 hours to develop or update a plan that is appropriate to the size of their organization. Based on this estimate, we believe that the overall cost for 25,644 EAS Participants to comply with the proposed certification requirement with 10 hours of labor from a General and Operations Manager who is compensated at $82 per hour will be $21,028,080. We seek comment on our analysis.

2. WEA Security

94. We propose to require Participating CMS Providers to certify that they are creating, annually updating, and implementing a cybersecurity risk management plan. As discussed above, WEA also faces security risks related to the transmission of false alerts and compromise of a Participating CMS Providers' systems could disrupt the transmission of a legitimate WEA message. Are there additional cybersecurity risks to WEA about which we should be aware? To what extent do Participating CMS Providers already have cybersecurity risk management plans? We believe that the approach we propose above in the context of EAS – wherein we would afford flexibility for providers to assess what content should be in their cybersecurity risk management plans while proposing that it demonstrate how the provider identifies the cyber risks that they face, the controls they use to mitigate those risks, and how they ensure that these controls are applied effectively to their operations – lends itself to WEA as well. We seek comment on this tentative conclusion. Are there any fundamental differences in the transmission of WEA alerts or the threats that WEA faces that would require a different approach to ensuring WEA's security? We seek comment on the least burdensome means by which Participating CMS Providers could submit their certification to the Commission, including via the Commission's Electronic Comment Filing System, a designated Commission e-mail address, or a WEA-specific database designed for this purpose.

95. As with the EAS, we propose that a cybersecurity risk management plan should include security controls sufficient to ensure the confidentiality, integrity, and availability of WEA. We propose sufficient security measures could be demonstrated by implementing controls like the CISA Cybersecurity Baseline or appropriate CIS Implementation Group. As with EAS Participants as described above we propose to require that each plan include a baseline of security measures that address changing default passwords prior to operation, installing security updates in a timely manner, securing equipment behind properly configured firewalls or using other segmentation practices, requiring multifactor authentication where applicable, addressing the replacement of end-of-life equipment, and wiping, clearing, or encrypting user information before disposing of old devices. We expect that compliant cybersecurity risk management plans will not be limited to only these specific measures, as plans will need regular updates to keep up with an evolving threat environment. We seek comment on these proposed rules. Are there specific security measures that we should require Participating CMS Providers to implement? For example, as above, we seek comment on whether we should require Participating CMS Providers to conduct network security audits or vulnerability assessments to identify potential security vulnerabilities, implement Incident Response Plans that describe the procedures that Participating CMS Providers would follow when responding to an ongoing cybersecurity incident, or require Participating CMS Providers to conduct cybersecurity training for their employees or contractors.

96. We believe that the benefits of this proposal for WEA outweighs the costs. As discussed above for EAS, we believe that the rules we propose today would better ensure that real WEA alerts with lifesaving information are successfully delivered to the public and false alerts are prevented in order to preserve public trust and better ensure that the public takes appropriate action during real emergencies. We estimate that the overall cost of our proposed cybersecurity risk management plan requirement will be approximately $62,320. We anticipate that many large Participating CMS Providers already have cybersecurity risk management plans

and will incur only de minimis costs to comply with this requirement. We also anticipate that many small Participating CMS Providers will require less than 10 hours to develop or update a plan that is appropriate to the size of their organization. Based on this estimate, we believe that the overall cost for 76 Participating CMS Providers to comply with the proposed certification requirement with 10 hours of labor from a General and Operations Manager who is compensated at $82 per hour will be $62,320. We seek comment on this analysis. To what extent do Participating CMS Providers already implement a cybersecurity risk management framework? Are there alternatives that would be as effective but less burdensome, particularly to smaller providers? As with EAS above, we seek comment on whether there are industry groups, cybersecurity organizations, or other organizations that may be positioned to help Participating CMS providers create, implement, and maintain their cybersecurity risk management plans. What kinds of resources do these organizations offer, and how can Participating CMS providers make use of them?

97. We seek comment on whether there are other categories of communications service providers (e.g., services that support 911 calling) to which a cybersecurity risk management plan certification requirement should apply. Like emergency alerting, 911 is part of the nation's emergency services critical infrastructure. Similarly, like the nation's alert and warning capability, 911 service has faced instances of compromise by cyberattacks, and is regularly under threat. In light of those threats, should services that support 911 calling also be required to annually certify to creating, updating, and implementing cybersecurity risk management plans? If so, are there differences between emergency alerting and 911 that would warrant changes to the risk management plan requirements we propose today, if applied to services that support 911 calling? Are the benefits and costs of such a requirement commensurate with the benefits and costs of certification as described above?

D. Displaying Only Valid WEA Messages on Mobile Devices

98. False alerts, such as the false ballistic missile alert that the Hawaii Emergency Management Agency accidentally sent during a training exercise in 2018, can cause panic, confusion, and damage the credibility of WEA. While that false alert was sent accidentally, bad actors could potentially exploit known WEA vulnerabilities to intentionally send false alerts to the public. The Commission's rules require Participating CMS Providers' network infrastructure to authenticate interactions with mobile devices and require mobile devices to authenticate interactions with CMS Provider infrastructure. In practice, however, the security handshake between Participating CMS Providers and mobile devices does not include a process for mobile devices to ensure that the base station to which it attaches is valid. As a result, mobile devices that are not actively engaged with a valid base station are vulnerable to receiving and presenting false alerts. This threat exists when a mobile device attempts authentication with the provider, switches base stations, or returns to active from idle mode.

99. Accordingly, we propose to require Participating CMS Providers transmit sufficient authentication information to allow mobile devices to present WEA alerts only if they come from valid base stations. Ongoing work in international standards bodies suggests that Participating CMS Providers could achieve this outcome by transmitting sufficient authentication information to allow mobile devices to authenticate either the alert or the base station itself. For example, Participating CMS Providers could provide for authentication of the base station using a unique identifier or an encryption key. To what extent do Participating CMS Providers already uniquely identify legitimate base stations with a selection of base station characteristics to defend against denial-of-service attacks and fraud (i.e., through base station fingerprinting)? Could Participating CMS Providers leverage base station fingerprinting to protect the public from false WEA alerts through updates to WEA standards and mobile device firmware? Alternatively, or in addition, could WEA-capable mobile devices receive an appropriate encryption key from the network and then use that key to confirm either that an alert is authentic or that the base station transmitting it is authentic before presenting the alert? Should our rules prohibit CMS Providers

and equipment manufacturers from marketing devices as WEA-capable unless they have these technical capabilities?

100. We seek comment on the trade-offs attendant to available technological approaches to protecting the public from false alerts. Could implementation of these approaches affect the ability of non-service initialized WEA-capable mobile devices, SIM-less WEA-capable mobile devices, or mobile devices that are no longer contractually associated with a CMS Provider to receive WEA alerts depending on the handset technology or generation of wireless network used? If so, how could the Commission mitigate these potential drawbacks by refining its proposed rules? To the extent that technological solutions have been implemented, is it still possible for a false alert of this type to be displayed on mobile devices, and if so, under what conditions? What steps could be taken to further minimize or eliminate these kinds of false alerts?

101. We estimate that Participating CMS Providers would incur a $14.5 million one-time cost to update the WEA standards and software necessary to comply with this requirement. This figure consists of approximately a $814,000 cost to update applicable WEA standards and approximately a $13.7 million cost to update applicable software. We quantify the cost of modifying standards as the annual compensation for 30 network engineers compensated at the national average for their field ($120,650/year; $58/hour), plus annual benefits ($60,325/year; 29/hour) working for the amount of time that it takes to develop a standard (one hour every other week for one year, 26 hours) for 12 distinct standards. We quantify the cost of modifying software as the annual compensation for a software developer compensated at the national average for their field ($120,990/year), plus annual benefits ($60,495/year) working for the amount of time that it takes to develop software (one year) at each of the 76 CMS Providers that participate in WEA. We seek comment on these cost estimates and the underlying cost methodology we are using. We also seek comment on any other costs and benefits that would result from this proposal. Incidents of false WEA alerts can cause significant confusion and

diminish the public's trust in emergency alerts. For example, what harms could arise if an invalid base station sends a false alert to attendees to a public event, such as a parade or sporting event? For each technological approach considered, we urge commenters to address its effectiveness and cost of implementation, any additional latency that the measure could introduce into the delivery of WEA alerts, and the potential for the security measure to result in the suppression of legitimate alert content.

E. WEA Infrastructure Functionality

102. Pursuant to the WARN Act, CMS Providers' participation in WEA is voluntary, but CMS Providers that elect to participate in WEA must comply with all the WEA rules. The WEA rules provide that WEA functionality, both in Participating CMS Providers' networks and in mobile devices, "are dependent upon the capabilities of the delivery technologies implemented by a Participating CMS Provider" and certain WEA protocols "are defined and controlled by each Participating CMS Provider." The inclusion of these statements may create the mistaken impression that Participating CMS Providers' compliance with the rules that follow, including the base station authentication rules we propose today, would be conditioned on the Participating CMS Providers' delivery technology. Emergency management agencies expect WEA to work as intended and when needed, and this language unintentionally could create uncertainties about the quality of WEA service that Participating CMS Providers offer. For these reasons, the Commission proposed to remove this language from the WEA rules in 2016. T-Mobile, ATIS, and CTIA, the only three commenters addressing this proposal, urged the Commission not to adopt it because "the rules should maximize the technological flexibility of CMS Providers participating in WEA." In the ten years since WEA's deployment, however, Participating CMS Providers have coalesced around cell broadcast as the wireless technology used to transmit WEA alerts to capable mobile devices, and ATIS has standardized system performance.

103. Accordingly, we seek to refresh the record on our proposal to remove these statements from the WEA rules. We believe these provisions introduce confusion and are

unnecessary, particularly as we do not expect that any Participating CMS Provider would need to make changes to their WEA service as a result of this proposed amendment. We seek comment on this proposal, particularly from any CMS Provider that would need to make changes to their WEA offerings in the event that the rules were so amended.

F. Promoting Digital Equity

104. The Commission, as part of its continuing effort to advance digital equity for all, including people of color, persons with disabilities, persons who live in rural or Tribal areas, and others who are or have been historically underserved, marginalized, or adversely affected by persistent poverty or inequality, invites comment on any equity-related considerations and benefits (if any) that may be associated with the proposals and issues discussed herein. Specifically, we seek comment on how our proposals may promote or inhibit advances in diversity, equity, inclusion, and accessibility, as well the scope of the Commission's relevant legal authority.

G. Compliance Timeframes

105. *Promoting the Operational Readiness of EAS Equipment*. To the extent that we adopt requirements to improve the operational readiness of EAS, we seek comment on when those rules should go into effect. For example, if we were to adopt rules to hasten or improve the Commission's visibility into the repair or replacement of non-operational EAS equipment, should those rules go into effect 30 days from publication in the *Federal Register* of notice that the Office of Management and Budget has completed its review of the modified information collection? What factors should we consider when determining when alternative operational readiness requirements should go into effect?

106. *Improving Awareness of Unauthorized Access to EAS Equipment.* We propose that the revision of § 11.45 to require EAS Participants to report any incident of unauthorized access of their EAS equipment would be effective 60 days from publication in the *Federal*

Register of notice that the Office of Management and Budget has completed its review of the modified information collection. We seek comment on this proposed timeframe. In the NDAA21 R&O, the Commission required EAS Participants to report false alerts to the Commission and, in a subsequent Public Notice, announced a compliance deadline approximately 60 days from publication in the *Federal Register* of notice that the Office of Management and Budget has approved the modified information collection. We seek comment on whether an EAS Participant's process for ascertaining whether an incident of unauthorized access of its EAS equipment has occurred and reporting it to the Commission entails a level of effort comparable to compliance with the Commission's false alert reporting requirement. Would EAS Participants' compliance with the Commission's false alert reporting requirement reduce the incremental burden of compliance with this proposal?

107. *Certifying to the Implementation of Cybersecurity Risk Management Plans*. We propose that EAS Participants and Participating CMS Providers must certify to the implementation of a cybersecurity risk management plan that includes measures sufficient to ensure the confidentiality, integrity, and reliability of their respective alerting systems within 12 months of the publication in the *Federal Register* of notice that the Office of Management and Budget has completed its review of the modified information collection. A 12-month timeframe would be intended to provide time for EAS Participants that do not already have a risk management plan in place to create one, including by preparing the organization to manage security and privacy risks, categorizing the systems and the information that it processes, stores, and transmits, and selecting controls to protect the system. A 12-month timeframe could also provide time to implement the security controls that the plan describes, assess whether the controls are in place, operating as intended, and producing the desired results, appoint a senior official to authorize the system, and develop mechanisms to continuously monitor control implementation and risks to the system. We seek comment on these proposals. Should we offer EAS Participants and Participating CMS Providers who are small businesses an additional 12

months to comply with this requirement, with compliance required within 24 months of publication in the *Federal Register* of notice that the Office of Management and Budget has completed its review of the modified information collection? Is there any reason why EAS and Participating CMS Providers should have different implementation timeframes?

108. *Displaying Only Valid WEA Messages on Mobile Devices*. We propose that CMS Providers transmit sufficient authentication information to allow mobile devices to present WEA alerts only if they come from valid base stations 30 months from the publication of these rules in the *Federal Register*. The record in our WEA proceedings supports the premise that Participating CMS Providers require 12 months to work through appropriate industry bodies to publish relevant standards, another 12 months for Participating CMS Providers and mobile device manufacturers to develop, test, and integrate software upgrades consistent with those standards, and then 6 more months to deploy this new technology to the field during normal technology refresh cycles. We seek comment on the applicability of this approach and timeframe, with which Participating CMS Providers have experience, to this proposal. We seek comment, in the alternative, on whether the urgent public safety need to protect the public from false alerts necessitates an expedited compliance timeframe and, if so, what that compliance timeframe should be.

109. *WEA Infrastructure Functionality*. We propose to remove language from our WEA infrastructure and mobile device rules effective 30 days after the rules' publication in the *Federal Register*. We do not believe that Participating CMS Providers will need to make any changes to comply with these rules as revised because they offer a WEA service that is consistent with the rules as otherwise written. We seek comment on this compliance timeframe and on this view.

III. Ordering Clauses

110. Accordingly, IT IS ORDERED that pursuant to sections 1, 2, 4(i), 4(n), 301, 303(b), 303(g), 303(r), 303(v), 307, 309, 335, 403, 624(g), and 706 of the Communications Act

of 1934, as amended, 47 U.S.C. 151, 152, 154(i), 154(n), 301, 303(b), 303(g), 303(r), 303(v), 307, 309, 335, 403, 544(g), and 606; The Warning, Alert and Response Network (WARN) Act, WARN Act sections 602(a), (b), (c), (f), 603, 604, and 606, 47 U.S.C. 1202(a), (b), (c), (f), 1203, 1204 and 1206; the Wireless Communications and Public Safety Act of 1999, Pub. L. 106-81, 47 U.S.C. 615, 615a, 615b; Section 202 of the Twenty-First Century Communications and Video Accessibility Act of 2010, as amended, 47 U.S.C. 613, this Notice of Proposed Rulemaking IS hereby ADOPTED.

List of Subjects

47 CFR part 10

Communications common carriers, Radio.

47 CFR part 11

Radio, Television.

Federal Communications Commission

Marlene Dortch,

Secretary.

For the reasons discussed in this preamble, the Federal Communications Commission proposes to amend 47 CFR parts 10 and 11 as follows:

PART 10 – WIRELESS EMERGENCY ALERTS

1. The authority citation for part 10 continues to read as follows:

Authority: 47 U.S.C. 151, 154(i) and (o), 201, 303(r), 403, and 606, 1202(a), (b), (c), (f), 1203, 1204, and 1206.

2. Revise § 10.330 to read as follows:

§ 10.330 Provider infrastructure requirements.

This section specifies the general functions that a Participating CMS Provider is required to perform within its infrastructure.

(a) Distribution of Alert Messages to mobile devices.

(b) Authentication of interactions with mobile devices**,** including the transmission of sufficient authentication information to allow mobile devices to only present WEA alerts from valid base stations.

(c) Reference Points D & E. Reference Point D is the interface between a CMS Provider gateway and its infrastructure. Reference Point E is the interface between a provider's infrastructure and mobile devices including air interfaces.

3. Add § 10.360 to subpart C to read as follows:

§ 10.360 Cybersecurity Risk Management Plan Certification.

(a) Each participating CMS Provider shall submit a certification to the Commission that it has created, annually updated, and implemented a cybersecurity risk management plan. The cybersecurity risk management plan shall describe how the Participating CMS Provider employs

its organizational resources and processes to ensure the confidentiality, integrity, and availability of WEA. The plan shall discuss how the Participating CMS Provider identifies the cyber risks that it faces, the controls it uses to mitigate those risks, and how it ensures that these controls are applied effectively to its operations. The plan shall address the security of all aspects of the Participating CMS Provider's communications systems and services that potentially could affect its provision of WEA messages. The plan shall be made available to the Commission upon request.

(b) Participating CMS Providers shall employ sufficient security controls to ensure the confidentially, integrity, and availability of the EAS. In furtherance of this requirement, the cybersecurity risk management plan shall address, but not be limited to, the following security controls:

(1) Changing default passwords prior to operation;

(2) Installing security updates in a timely manner;

(3) Securing equipment behind properly configured firewalls or using other segmentation practices;

(4) Requiring multifactor authentication where applicable;

(5) Addressing the replacement of end-of-life equipment; and

(6) Wiping, clearing, or encrypting user information before disposing of old devices.

(c) Participating CMS Providers shall take reasonable measures to protect the confidentiality, integrity, and availability of EAS to avoid the transmission of false alerts or non-transmission of valid Alert Messages; failure to do so shall be, in addition to a violation of any specific provisions of this section, § 11.45(a) of this chapter, or § 10.520(d), an independent breach of this duty.

4. Revise § 10.500 introductory text as follows:

§ 10.500 General requirements.

Mobile devices are required to perform the following functions:

* * * * *

PART 11 – EMERGENCY ALERT SYSTEM (EAS)

5. The authority citation for part 11 continues to read as follows:

Authority: 47 U.S.C. 151, 154 (i) and (o), 303(r), 544(g), 606, 1201, 1206.

6. Amend § 11.35 by adding paragraph (d) to read as follows:

§ 11.35 Equipment operational readiness.

* * * * *

(d) Annual EAS Security Certification.

(1) The identifying information required by the ETRS as specified in §11.61(a)(3)(iv) shall include a Certification to the Commission that the EAS Participant has created, annually updated, and implemented a cybersecurity risk management plan. The cybersecurity risk management plan shall describe how the EAS Participant employs its organizational resources and processes to ensure the confidentiality, integrity, and availability of the EAS. The plan shall discuss how the EAS Participant identifies the cyber risks that its faces, the controls it uses to mitigate those risks, and how it ensures that these controls are applied effectively to their operations. The plan shall address the security of all aspects of an EAS Participant's communications systems and services that potentially could affect its provision of EAS messages. The plan shall be made available to the Commission upon request.

(2) EAS Participants shall employ sufficient security controls to ensure the confidentially, integrity, and availability of the EAS. In furtherance of this requirement, the cybersecurity risk management plan shall address, but not be limited to, the following

security controls:

(i) Changing default passwords prior to operation;

(ii) Installing security updates in a timely manner;

(iii) Securing equipment behind properly configured firewalls or using other segmentation practices;

(iv) Requiring multifactor authentication where applicable;

(v) Addressing the replacement of end-of-life equipment; and

(vi) Wiping, clearing, or encrypting user information before disposing of old devices.

(3) EAS Participants shall take reasonable measures to protect the confidentiality, integrity, and availability of EAS to avoid the transmission of false alerts or non-transmission of valid EAS messages; failure to do so shall be, in addition to a violation of any specific provisions of this section, § 11.45(a), or § 10.520(d) of this chapter, an independent breach of this duty.

7. Amend § 11.45 by redesignating paragraph (c) as paragraph (d) and adding a new paragraph (c) to read as follows:

§ 11.45 Prohibition of false or deceptive EAS transmissions.

* * * * *

(c) No later than seventy-two (72) hours after an EAS Participant knows or should have known that its EAS equipment, or communications systems, or services that potentially could affect their provision of EAS, have been accessed in an unauthorized manner, the EAS Participant shall provide notification to the Commission identifying, if applicable, the date range of the incident, a description of the unauthorized access, the impact to the EAS Participant's EAS operational readiness, a description of the vulnerabilities exploited and the techniques used to access the device, identifying information for each actor responsible for the incident, and

contact information for the EAS Participant. When one event or set of events gives rise to obligations under both paragraphs (b) and (c) of this section, an EAS Participant remains subject to each requirement individually. The Participant may elect to send a single notification to the Commission within 24 hours providing all the information described in both paragraphs or separate notification to the Commission within 24 hours and 72 hours.

* * * * *

[FR Doc. 2022-25263 Filed: 11/22/2022 8:45 am; Publication Date: 11/23/2022]